ON REPRESENTATION OF INTEGERS BY BINARY QUADRATIC FORMS IN ALGEBRAIC NUMBER FIELDS

by

STIG CHRISTOFFERSON

UPPSALA 1962

ALMQVIST & WIKSELLS BOKTRYCKERI AB

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548912_0003

ON REPRESENTATION OF INTEGERS BY BINARY QUADRATIC FORMS IN ALGEBRAIC NUMBER FIELDS

INAUGURAL DISSERTATION

by

STIG CHRISTOFFERSON
Fil. lic., Norrl.

BY DUE PERMISSION OF THE FACULTY
OF MATHEMATICS AND SCIENCE OF THE UNIVERSITY
OF UPPSALA, TO BE PUBLICLY DISCUSSED AT THE
LECTURE ROOM OF THE INSTITUTE
FOR THEORETICAL PHYSICS,
MAY 11TH, 1962, AT 10 A.M.,
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UPPSALA 1962

ALMQVIST & WIKSELLS BOKTRYCKERI AB

R.UNIV.
HIBLIOTHEEK
LEIDEN

ON REPRESENTATION OF INTEGERS BY BINARY QUADRATIC FORMS IN ALGEBRAIC NUMBER FIELDS

by

STIG CHRISTOFFERSON

UPPSALA 1962

ALMQVIST & WIKSELLS BOKTRYCKERI AB

R. UNIV.
BIBLIOTHEEK
LEIDEN

I wish to express my deep gratitude to my distinguished teacher, Professor Trygve Nagell, who suggested the theme of this thesis and has followed my work with stimulating interest.

My thanks are further due to Mrs. Elaine Svenonius, who revised the English text.

Uppsala, April 1962. *Stig Christofferson*

INTRODUCTION

The study of representation of integers by quadratic forms (especially binary forms) belongs to classical number theory. Already Fermat showed such results as the following: Every prime of the type $8n+1$ can be represented by the form x^2+2y^2 for x and y integers. Later Gauss and others, especially Dirichlet, extensively studied arithmetic properties of quadratic forms. In our century some parts of the general theory have become in a way very complete due to Hasse's results making use of p-adic numbers, and those of Siegel obtained by the use of analytical methods. They also consider quadratic forms in algebraic number fields, giving generalizations of the theory in the rational field (see Hasse [1] and Siegel [9]).

But it is still often a difficult problem to decide what integers are representable by a given quadratic form. Nagell has in the papers [6], [7] and [8] discussed the special binary quadratic form x^2+y^2, mainly in certain quadratic number fields. The purpose of this thesis is to generalize some of Nagell's results.

In the first chapter I study the number of representations of integers ω by a quadratic form

$$\omega = \alpha\xi^2 + \beta\xi\eta + \gamma\eta^2$$

in an algebraic number field $\mathbf{\Omega}$; α, β, γ, ξ and η are integers in $\mathbf{\Omega}$ such that $\delta = 4\alpha\gamma - \beta^2 \neq 0$. The main result is that in most fields $\mathbf{\Omega}$ any integer that has one representation by this form has infinitely many. The exceptional cases are those fields $\mathbf{\Omega}$ for which the field $\mathbf{\Omega}(\sqrt{-\delta})$ is rational or quadratic imaginary, and those fields that are totally real with δ totally positive. In these cases no integer has infinitely many representations. Use is made of Dirichlet's theorem about the number of fundamental units in an algebraic field. I also give some results about automorphs of quadratic forms in $\mathbf{\Omega}$.

In the second and last chapter I investigate representations by the form

$$\xi^2 + D\eta^2$$

in the gaussian number field $\mathbf{K}(\sqrt{-1})$, where D assumes certain rational integral values that make the fields $\mathbf{K}(\sqrt{D})$ and $\mathbf{K}(\sqrt{-D})$ simple fields.

For these values of D I give a complete characterization of those integers in $\mathbf{K}(\sqrt{-1})$ that can be represented by the form. The proofs of the results depend upon simple properties of relatively quadratic fields and especially properties of the Dirichlet field $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$. In this chapter I also give a remark on some results in Nagell [6].

CHAPTER I

ON THE NUMBER OF REPRESENTATIONS

1. Definitions

Let α, β and γ be integers in an algebraic number field $\mathbf{\Omega}$. We put $\delta = 4\alpha\gamma - \beta^2$ and suppose $\delta \neq 0$. If an integer $\omega \neq 0$ in $\mathbf{\Omega}$ can be written

$$\omega = \alpha\xi^2 + \beta\xi\eta + \gamma\eta^2$$

with integers ξ and η in $\mathbf{\Omega}$ we say that ω is an (α, β, γ)-NUMBER in $\mathbf{\Omega}$ and we call (ξ, η) an (α, β, γ)-REPRESENTATION of ω in $\mathbf{\Omega}$.

In this chapter we want to prove as the main result that every (α, β, γ)-number in $\mathbf{\Omega}$ has infinitely many (α, β, γ)-representations in $\mathbf{\Omega}$ except when $\mathbf{\Omega}(\sqrt{-\delta})$ is the rational field or an imaginary quadratic field and when $\mathbf{\Omega}$ is a totally real field with δ totally positive. In these exceptional cases every (α, β, γ)-number has finitely many (α, β, γ)-representations.

We start by considering representations by the form

$$\xi^2 + \delta\eta^2$$

and instead of the terms $(1, 0, \delta)$-number and $(1, 0, \delta)$-representation we simply use δ-NUMBER and δ-REPRESENTATION. We call (ξ, η) a TRIVIAL REPRESENTATION if and only if $\xi\eta = 0$.

2. Representations by $\xi^2 + \delta\eta^2$

Lemma 1. *The number* 1 *has infinitely many* δ*-representations in* $\mathbf{\Omega}$ *if and only if it has a non-trivial* δ*-representation in* $\mathbf{\Omega}$.

Proof. As there can be at most four trivial representations the only-if part of the lemma is obvious.

Suppose there is a non-trivial representation

$$1 = \xi^2 + \delta\eta^2,$$

where ξ, η and δ are integers $\neq 0$ in $\mathbf{\Omega}$. Then fix a value $\sqrt{-\delta}$ and put for $n = 0, 1, 2, 3, \ldots$

$$\xi_n + \eta_n \sqrt{-\delta} = (\xi + \eta \sqrt{-\delta})^n,$$

where

$$\begin{cases} \xi_n = \xi^n - \binom{n}{2} \delta \xi^{n-2} \eta^2 + \binom{n}{4} \delta^2 \xi^{n-4} \eta^4 - \ldots, \\ \eta_n = \binom{n}{1} \xi^{n-1} \eta - \binom{n}{3} \delta \xi^{n-3} \eta^3 + \ldots. \end{cases} \tag{1}$$

The numbers ξ_n and η_n are integers in $\mathbf{\Omega}$ and

$$\xi_n - \eta_n \sqrt{-\delta} = (\xi - \eta \sqrt{-\delta})^n.$$

Hence

$$\xi_n^2 + \delta \eta_n^2 = 1,$$

i.e. (ξ_n, η_n), $n = 0, 1, 2, \ldots$, are δ-representations of the number 1 in $\mathbf{\Omega}$. We want to show that they are all different. It follows from $\xi_m + \eta_m \sqrt{-\delta} = \xi_n + \eta_n \sqrt{-\delta}$ that $\xi + \eta \sqrt{-\delta}$ must be a root of unity ϱ, such that

$$\xi = \frac{1}{2}(\varrho + \varrho^{-1}), \quad \eta = \frac{1}{2\sqrt{-\delta}}(\varrho - \varrho^{-1}).$$

In Nagell [6], p. 52, it is shown that these values of ξ and $\eta \sqrt{-\delta}$ cannot be integers with $\xi\eta \neq 0$ if ϱ is a root of unity. Hence Lemma 1 is proved.

Lemma 2. *A δ-number has infinitely many δ-representations in $\mathbf{\Omega}$ if and only if the number 1 has a non-trivial δ-representation in $\mathbf{\Omega}$.*

Proof. Let ω be a δ-number in $\mathbf{\Omega}$,

$$\omega = \mu^2 + \delta \nu^2,$$

and suppose the number 1 has a non-trivial δ-representation. Then the number 1 has infinitely many δ-representations given by (1). Put

$$\mu_n + \nu_n \sqrt{-\delta} = (\mu + \nu \sqrt{-\delta})(\xi_n + \eta_n \sqrt{-\delta}), \quad n = 0, 1, 2, \ldots,$$

where

$$\mu_n = \mu \xi_n - \delta \nu \eta_n \quad \text{and} \quad \nu_n = \mu \eta_n + \nu \xi_n.$$

(μ_n, ν_n), $n = 0, 1, 2, \ldots$, are δ-representations of ω and they are all different.

Now suppose ω has infinitely many δ-representations

$$\omega = \mu_n^2 + \delta\nu_n^2, \quad n = 1, 2, 3, \ldots. \tag{2}$$

It is no restriction to assume $\mu_n\nu_n \neq 0$ for all n and

$$\mu_m \neq \pm\mu_n \quad \text{for} \quad m \neq n. \tag{3}$$

If $\sqrt{\delta}$ is a unit in $\mathbf{\Omega}$ we also can assume

$$\mu_m \neq \pm\nu_n\sqrt{\delta} \quad \text{for} \quad m \neq n. \tag{4}$$

In $\mathbf{\Omega}$ there are only finitely many residue classes modulo the principal ideal (ω). Hence there exist representations (2) such that

$$\mu_m \equiv \mu_n \pmod{\omega} \quad \text{and} \quad \nu_m \equiv \nu_n \pmod{\omega}$$

with $m \neq n$. Then

$$\omega^2 = (\mu_m^2 + \delta\nu_m^2)(\mu_n^2 + \delta\nu_n^2) = (\mu_m\mu_n + \delta\nu_m\nu_n)^2 + \delta(\mu_m\nu_n - \mu_n\nu_m)^2.$$

Now
$$\begin{cases} \omega\xi = \mu_m\mu_n + \delta\nu_m\nu_n \equiv 0 \pmod{\omega}, \\ \omega\eta = \mu_m\nu_n - \mu_n\nu_m \equiv 0 \pmod{\omega}, \end{cases}$$

and hence $1 = \xi^2 + \delta\eta^2$ with integers ξ and η in $\mathbf{\Omega}$.

(ξ, η) is a non-trivial representation. For if $\eta = 0$ then $\nu_n = \mu_n\nu_m\mu_m^{-1}$ and

$$\pm\omega = \mu_m\mu_n + \delta\nu_m^2\mu_n\mu_m^{-1} = \mu_n\mu_m^{-1}\omega$$

contrary to assumption (3). $\xi = 0$ is impossible because of (4). This completes the proof of Lemma 2.

The result of Lemma 2 can also be stated in the following way: *Every δ-number has infinitely many δ-representations in $\mathbf{\Omega}$ if and only if there exists one δ-number with infinitely many δ-representations in $\mathbf{\Omega}$.*

3. Representations by $\alpha\xi^2 + \beta\xi\eta + \gamma\eta^2$

We now turn to (α, β, γ)-representations in $\mathbf{\Omega}$. In this section we consider the case when *not both α and γ are equal to* 0. As it is no restriction we put $\alpha \neq 0$. With $\delta = 4\alpha\gamma - \beta^2$ we have

$$\alpha\xi^2 + \beta\xi\eta + \gamma\eta^2 = (4\alpha)^{-1}[(2\alpha\xi + \beta\eta)^2 + \delta\eta^2].$$

If ω is an (α, β, γ)-number in $\mathbf{\Omega}$ with infinitely many (α, β, γ)-repre-

sentations then $4\alpha\omega$ has infinitely many δ-representations in Ω, which implies that the number 1 has a non-trivial δ-representation. This proves the only-if part of the following theorem.

Theorem 1. *Let α, β and γ be integers in an algebraic number field Ω so that α and γ are not both 0 and $\delta = 4\alpha\gamma - \beta^2 \neq 0$. Then an (α, β, γ)-number has infinitely many (α, β, γ)-representations in Ω if and only if the number 1 has a non-trivial δ-representation in Ω.*

Proof. Suppose the number 1 has the δ-representations (1) and let ω be an (α, β, γ)-number,

$$\omega = \alpha\mu^2 + \beta\mu\nu + \gamma\nu^2,$$

and

$$4\alpha\omega = (2\alpha\mu + \beta\nu)^2 + \delta\nu^2.$$

According to Lemma 2 the δ-number $4\alpha\omega$ has infinitely many δ-representations (σ_n, τ_n), $n = 0, 1, 2, \ldots$, given by

$$\begin{cases} \sigma_n = (2\alpha\mu + \beta\nu)\,\xi_n - \delta\nu\eta_n, \\ \tau_n = (2\alpha\mu + \beta\nu)\,\eta_n + \nu\xi_n. \end{cases}$$

Now if

$$\begin{cases} \mu_n = \mu\xi_n - (\beta\mu + 2\gamma\nu)\,\eta_n, \\ \nu_n = \nu\xi_n + (2\alpha\mu + \beta\nu)\,\eta_n, \end{cases}$$

then

$$\sigma_n = 2\alpha\mu_n + \beta\nu_n \quad \text{and} \quad \tau_n = \nu_n.$$

Hence (μ_n, ν_n) is an (α, β, γ)-representation of ω in Ω. For different values of n the representations are different. Hence there are infinitely many (α, β, γ)-representations of ω in Ω and the theorem is proved.

The result can also be stated in the following way: *Every (α, β, γ)-number has infinitely many (α, β, γ)-representations in Ω if and only if there exists one (α, β, γ)-number with infinitely many (α, β, γ)-representations.*

It is also possible to show that Theorem 1 still holds if both α and γ are allowed to be equal to 0, but we postpone this discussion until the proof of Theorem 3.

4. Conditions on Ω and δ for a non-trivial δ-representation of the number 1 in Ω

Next we want to investigate under what conditions the number 1 has a non-trivial δ-representation in Ω and thus infinitely many. From

$$1 = \xi^2 + \delta\eta^2 = (\xi + \eta\sqrt{-\delta})(\xi - \eta\sqrt{-\delta})$$

it follows that a necessary condition is that the field $\Omega_1 = \Omega(\sqrt{-\delta})$ has *infinitely many units*. Hence if Ω_1 is the rational field $\mathbf{K}(1)$ or an imaginary quadratic field there are only trivial representations of the number 1.

If $\Omega_1 = \mathbf{K}(1)$ then $\Omega = \mathbf{K}(1)$ and $-\delta$ is the square of a rational integer.

If Ω_1 is imaginary quadratic then one of the following cases occurs:

1°. $\Omega = \mathbf{K}(1)$ and δ is a positive rational integer;

2°. Ω is imaginary quadratic and $-\delta$ is the square of an integer in Ω.

There is one more case with only trivial representations of the number 1, and that is when Ω is *totally real* and δ *totally potitive*. Suppose in this case

$$1 = \xi^2 + \delta\eta^2, \ \xi \text{ and } \eta \text{ integers in } \Omega.$$

Then $$1 = \xi^{(i)2} + \delta^{(i)}\eta^{(i)2}, \ \xi^{(i)} \text{ and } \eta^{(i)} \text{ integers in } \Omega^{(i)}.$$

Here $\Omega^{(1)}, \ldots, \Omega^{(n)}$ are the conjugate fields of Ω, and $\delta^{(i)}$, $\xi^{(i)}$, $\eta^{(i)}$ are the conjugates in $\Omega^{(i)}$ of δ, ξ, η respectively. If $\eta \neq 0$, then $\delta^{(i)}\eta^{(i)2} > 0$ and $\xi^{(i)2} < 1$. Then for the norm $N(\xi)$ of ξ it follows that

$$|N(\xi)| = |\xi^{(1)} \ldots \xi^{(n)}| < 1,$$

which implies $N(\xi) = 0$ and $\xi = 0$. Thus there is no non-trivial δ-representation of the number 1.

The following theorem ensures that there are no other cases with only trivial δ-representations of the number 1.

Theorem 2. *The number* 1 *has a non-trivial* δ*-representation in* Ω *except in the following cases:*

1°. $\Omega(\sqrt{-\delta})$ *is the rational field or an imaginary quadratic field;*

2°. Ω *is totally real and* δ *totally positive.*

Proof. Let δ and Ω be such that none of the exceptional cases holds. Then $\Omega(\sqrt{-\delta})$ has at least one fundamental unit. We shall distinguish between two cases.

I. $\sqrt{-\delta}$ belongs to Ω, i.e. $\Omega(\sqrt{-\delta}) = \Omega$.

Let ε be a unit in Ω that is not a root of unity. Put

$$\xi = \frac{\varepsilon^m + \varepsilon^{-m}}{2} \quad \text{and} \quad \eta = \frac{\varepsilon^m - \varepsilon^{-m}}{2\sqrt{-\delta}}. \tag{5}$$

Then for every rational integer m the numbers ξ and η belong to $\mathfrak{Q}$ and $\xi^2 + \delta\eta^2 = 1$. ξ and η are integers if $m = \Phi(2\sqrt{-\delta})$, where $\Phi(2\sqrt{-\delta})$ denotes the number of residue classes modulo $2\sqrt{-\delta}$ in $\mathfrak{Q}$ which are prime to $2\sqrt{-\delta}$. $\xi\eta \neq 0$ because ε is not a root of unity. Hence (ξ, η) is a non-trivial δ-representation of the number 1 in $\mathfrak{Q}$.

II. $\sqrt{-\delta}$ does not belong to $\mathfrak{Q}$.

In this case (5) does not give a representation in $\mathfrak{Q}$ if ε belongs to $\mathfrak{Q}$.

i) First suppose the number of fundamental units is greater in $\mathfrak{Q}(\sqrt{-\delta})$ than in $\mathfrak{Q}$. We can then find a unit E in $\mathfrak{Q}(\sqrt{-\delta})$ that does not belong to $\mathfrak{Q}$ and such that E^2 is not the product of a unit in $\mathfrak{Q}$ and a root of unity. Put $E = \varphi + \psi\sqrt{-\delta}$, where φ and ψ (not necessarily integers) belong to $\mathfrak{Q}$. Then $E_1 = \varphi - \psi\sqrt{-\delta}$ is also a unit in $\mathfrak{Q}(\sqrt{-\delta})$ and $EE_1 = \varphi^2 + \delta\psi^2$ is a unit in $\mathfrak{Q}$. Put

$$\xi = \frac{E^{2m} + E_1^{2m}}{2(EE_1)^m} \quad \text{and} \quad \eta = \frac{E^{2m} - E_1^{2m}}{2(EE_1)^m\sqrt{-\delta}}.$$

Then ξ and η belong to $\mathfrak{Q}$ and $\xi^2 + \delta\eta^2 = 1$. If $m = \Phi(2\sqrt{-\delta})$ in $\mathfrak{Q}(\sqrt{-\delta})$ then ξ and η are integers. $\xi\eta = 0$ implies that $E^2(\varphi^2 + \delta\psi^2)^{-1}$ is a root of unity contrary to the assumption on E. Hence (ξ, η) is a non-trivial δ-representation of the number 1 in $\mathfrak{Q}$.

ii) Suppose $\mathfrak{Q}$ and $\mathfrak{Q}(\sqrt{-\delta})$ have the same number of fundamental units. If $\mathfrak{Q}$ has r_1 real and $2r_2$ imaginary conjugate fields, then the degree of $\mathfrak{Q}$ is $n = r_1 + 2r_2$ and the number of fundamental units is $r = r_1 + r_2 - 1$. Let the corresponding numbers for $\mathfrak{Q}(\sqrt{-\delta})$ be R_1, R_2 and R. Then $2n = R_1 + 2R_2$ and $R = R_1 + R_2 - 1$. If the conjugate fields $\mathfrak{Q}^{(i)}$ are generated by $\theta^{(i)}$, $i = 1, 2, \ldots, n$, then the conjugate fields of $\mathfrak{Q}(\sqrt{-\delta})$ are generated by the $2n$ numbers

$$\theta^{(i)} \pm h\sqrt{-\delta^{(i)}},$$

where h is a suitable rational integer.

Let r_1' be the number of the real conjugate fields $\mathfrak{Q}^{(i)}$ of $\mathfrak{Q}$ where the conjugate value $\delta^{(i)}$ of δ is negative, and let r_1'' be the number of the real fields $\mathfrak{Q}^{(i)}$ with positive $\delta^{(i)}$. Then $r_1 = r_1' + r_1''$, $R_1 = 2r_1'$ and $R_2 = r_1'' + 2r_2$. $R = r$ implies

$$2r_1' + r_1'' + 2r_2 = r_1' + r_1'' + r_2,$$

and consequently $r_1' = r_2 = 0$. $r_2 = 0$ means that Ω is totally real and $r_1' = 0$ that δ is totally positive. But this case was excluded and the theorem is proved.

Theorem 3. *If α, β and γ are integers in an algebraic number field Ω so that $\delta = 4\alpha\gamma - \beta^2 \neq 0$, then every (α, β, γ)-number has infinitely many (α, β, γ)-representations in Ω except in the following cases:*

1°. *$\Omega(\sqrt{-\delta})$ is the rational field or an imaginary quadratic field;*

2°. *Ω is totally real and δ totally positive.*

In these two cases every (α, β, γ)-number has finitely many (α, β, γ)-representations.

Proof. If α and γ are not both equal to 0 then Theorems 1 and 2 immediately give Theorem 3.

If $\alpha = \gamma = 0$ we consider $(0, \beta, 0)$-representations

$$\omega = \beta\xi\eta, \quad \beta \neq 0.$$

Obviously ω is a $(0, \beta, 0)$-number if and only if ω is divisible by β. There are infinitely many $(0, \beta, 0)$-representations if and only if Ω contains infinitely many units. Hence the exceptional case is when Ω is the rational field or an imaginary quadratic field. Since $\delta = -\beta^2$ we have $\Omega(\sqrt{-\delta}) = \Omega$ which corresponds to case 1° in the theorem. Case 2° cannot occur, for if Ω is real then $\delta = -\beta^2$ is negative. Hence the theorem is true also for $\alpha = \gamma = 0$.

5. Automorphs of $\alpha\xi^2 + \beta\xi\eta + \gamma\eta^2$

If a transformation

$$\begin{cases} \xi = \pi\xi' + \varrho\eta' \\ \eta = \sigma\xi' + \tau\eta' \end{cases}$$

takes the quadratic form

$$f(\xi, \eta) = \alpha\xi^2 + \beta\xi\eta + \gamma\eta^2$$

into itself, i.e. so that identically

$$f(\pi\xi + \varrho\eta, \sigma\xi + \tau\eta) \equiv f(\xi, \eta), \tag{6}$$

we call the transformation an AUTOMORPH of the form $f(\xi, \eta)$. We shall mostly be concerned with automorphs, the coefficients of which are integers in the field $\mathbf{\Omega}$ in which (α, β, γ)-representations are studied. In this case the automorph is called an INTEGRAL AUTOMORPH in $\mathbf{\Omega}$. The automorph is called DIRECT or INDIRECT depending on whether $\pi\tau - \varrho\sigma$ is equal to 1 or -1.

The proof of Theorem 1 on the existence of infinitely many (α, β, γ)-representations of an (α, β, γ)-number in $\mathbf{\Omega}$ makes use of the existence of infinitely many integral automorphs in $\mathbf{\Omega}$. As a direct consequence of the way Theorem 3 was proved we can state the following result about the number of integral automorphs.

Theorem 4. *Let α, β and γ be integers in an algebraic number field $\mathbf{\Omega}$ so that $\delta = 4\alpha\gamma - \beta^2 \neq 0$. Then the quadratic form $\alpha\xi^2 + \beta\xi\eta + \gamma\eta^2$ has infinitely many integral automorphs in $\mathbf{\Omega}$ except in the following cases:*

1°. *$\mathbf{\Omega}(\sqrt{-\delta})$ is the rational field or an imaginary quadratic field;*

2°. *$\mathbf{\Omega}$ is totally real and δ totally positive.*

In the proof of Theorem 1 the automorphs of $\alpha\xi^2 + \beta\xi\eta + \gamma\eta^2$ were obtained by means of automorphs of $\xi^2 + (4\alpha\gamma - \beta^2)\eta^2$, but no effort was made to find all integral automorphs. If $\mathbf{\Omega}$ is the rational field the method for determining all direct integral automorphs is well known (see for instance Jones [5]). Use is there made of divisibility properties of the rational integers. However, some of the results carry over to the general case. We want to show that if the greatest common divisor $(\alpha, \beta, \gamma) = (1)$ then the *direct integral automorphs* are characterized in the same manner as in the rational case.

Let us first consider the form

$$F(\xi, \eta) = \xi^2 + \delta\eta^2; \quad \delta \neq 0.$$

Then (6) is equivalent to the system of equations

$$\begin{cases} \pi^2 + \delta\sigma^2 = 1 \\ \pi\varrho + \delta\sigma\tau = 0 \\ \varrho^2 + \delta\tau^2 = \delta. \end{cases} \tag{7}$$

From these equations it follows that

$$\pi^2\varrho^2 = \delta^2\sigma^2\tau^2 = (1 - \pi^2)(\delta - \varrho^2) = \delta - \varrho^2 - \delta\pi^2 + \pi^2\varrho^2 = \delta(\tau^2 - \pi^2) + \pi^2\varrho^2.$$

Hence
$$\tau = \pm\pi \quad \text{and} \quad \varrho = \mp\delta\sigma. \tag{8}$$

Conversely, if π and σ satisfy $\pi^2+\delta\sigma^2=1$ and if $\tau=\pm\pi$ and $\varrho=\mp\delta\sigma$, then all the equations (7) are satisfied, and moreover

$$\pi\tau-\varrho\sigma=\pm 1$$

with $+$ and $-$ corresponding to upper and lower signs in (8) respectively. We have then proved the following lemma.

Lemma 3. *The transformation*

$$\begin{cases}\xi=\pi\xi'+\varrho\eta'\\ \eta=\sigma\xi'+\tau\eta'\end{cases}$$

is an automorph of the form $\xi^2+\delta\eta^2$ $(\delta\neq 0)$ *if and only if* π, ϱ, σ *and* τ *satisfy*

$$\pi^2+\delta\sigma^2=1,\quad \tau=\pm\pi,\quad \varrho=\mp\delta\sigma.$$

The automorph is direct for the upper signs and indirect for the lower signs.

It should be noted that the proof of this lemma is of purely algebraic nature and does not use any number-theoretical properties of the coefficients in the quadratic form and in the automorph.

We now consider automorphs of the quadratic form

$$f(\xi,\eta)=\alpha\xi^2+\beta\xi\eta+\gamma\eta^2$$

with $$\delta=4\alpha\gamma-\beta^2\neq 0 \quad \text{and} \quad \alpha\neq 0.$$

Suppose we have an automorph of $f(\xi,\eta)$

$$\begin{cases}\xi=\pi\xi'+\varrho\eta'\\ \eta=\sigma\xi'+\tau\eta'.\end{cases}$$

Since $f(\xi,\eta)=(4\alpha)^{-1}[(2\alpha\xi+\beta\eta)^2+\delta\eta^2]$ the automorph of $f(\xi,\eta)$ will give an automorph of $F(\mu,\nu)=\mu^2+\delta\nu^2$, namely

$$\begin{cases}\mu=\left(\pi+\dfrac{\beta\sigma}{2\alpha}\right)\mu'+\left(2\alpha\varrho-\beta\pi-\dfrac{\beta^2\sigma}{2\alpha}+\beta\tau\right)\nu'\\ \nu=\dfrac{\sigma}{2\alpha}\mu'+\left(\tau-\dfrac{\beta\sigma}{2\alpha}\right)\nu'.\end{cases}$$

According to Lemma 3 this is an automorph of $\mu^2+\delta\nu^2$ if and only if

$$\begin{cases} \left(\pi+\dfrac{\beta\sigma}{2\alpha}\right)^2+\delta\left(\dfrac{\sigma}{2\alpha}\right)^2=1 \\ \tau-\dfrac{\beta\sigma}{2\alpha}=\pm\left(\pi+\dfrac{\beta\sigma}{2\alpha}\right) \\ 2\alpha\varrho-\beta\pi-\dfrac{\beta^2\sigma}{2\alpha}+\beta\tau=\mp\dfrac{\delta\sigma}{2\alpha}. \end{cases} \tag{9}$$

For the upper signs this system is equivalent to

$$\begin{cases} \alpha\pi^2+\beta\pi\sigma+\gamma\sigma^2=\alpha \\ \tau-\pi=\dfrac{\beta\sigma}{\alpha} \\ \alpha\varrho+\gamma\sigma=0, \end{cases}$$

which implies $$\pi\tau-\varrho\sigma=1.$$

The lower signs give $\pi\tau-\varrho\sigma=-1$ and we shall return to this case later.

If we put

$$\varphi=\pi+\frac{\beta\sigma}{2\alpha}, \qquad \psi=\frac{\sigma}{2\alpha},$$

we obtain

$$\begin{cases} \varphi^2+\delta\psi^2=1, \\ \pi=\varphi-\beta\psi, \quad \varrho=-2\gamma\psi, \\ \sigma=2\alpha\psi, \qquad \tau=\varphi+\beta\psi. \end{cases}$$

This system will give all automorphs of $f(\xi,\eta)$. We now want to find the automorphs having integer coefficients π, ϱ, σ and τ in the algebraic field $\mathbf{\Omega}$, supposing α, β and γ to be integers in $\mathbf{\Omega}$. Apparently every δ-representation (φ,ψ) of the number 1 in $\mathbf{\Omega}$ gives an integral automorph of $f(\xi,\eta)$ in $\mathbf{\Omega}$. But these are in general not the only integral automorphs.

If π, ϱ, σ and τ are integers then it follows that $2\varphi=\pi+\tau$ is an integer and also the numbers $2\alpha\psi$, $2\beta\psi$ and $2\gamma\psi$ are integers. Put $\psi=\psi_1/2\psi_2$ with ψ_1 and ψ_2 integers. Either ψ_2 divides ψ_1 or there is a prime ideal $\mathfrak{p}$ such that $\mathfrak{p}^n$ divides ψ_2 but not ψ_1 for some rational integer $n\geqq 1$. Then $\mathfrak{p}$ must divide α, β and γ.

Hence, if $(\alpha,\beta,\gamma)=(1)$, then we must have $\varphi=\frac{1}{2}\varphi_1$ and $\psi=\frac{1}{2}\psi_1$ with φ_1 and ψ_1 integers. Conversely, if φ and ψ have these values with $\varphi^2+\delta\psi^2=1$ then π, ϱ, σ and τ are all integers. With the assumption $\alpha\neq 0$ or $\gamma\neq 0$ the following theorem is then proved.

Theorem 5. *If α, β and γ are integers in an algebraic field Ω such that $\delta = 4\alpha\gamma - \beta^2 \neq 0$ and $(\alpha, \beta, \gamma) = (1)$, then*

$$\begin{cases} \xi = \pi\xi' + \varrho\eta' \\ \eta = \sigma\xi' + \tau\eta' \end{cases}$$

is a direct integral automorph of the quadratic form $\alpha\xi^2 + \beta\xi\eta + \gamma\eta^2$ if and only if

$$\pi = \tfrac{1}{2}(\varphi - \beta\psi), \quad \varrho = -\gamma\psi,$$

$$\sigma = \alpha\psi, \qquad \tau = \tfrac{1}{2}(\varphi + \beta\psi),$$

where (φ, ψ) is a δ-representation of 4 in Ω,

$$\varphi^2 + \delta\psi^2 = 4.$$

In the above proof of the theorem we assumed $\alpha \neq 0$ or $\gamma \neq 0$. The integral automorphs of

$$\beta\xi\eta$$

can easily be completely determined. They are

$$\begin{cases} \xi = \varepsilon\xi', \\ \eta = \varepsilon^{-1}\eta', \end{cases} \quad \text{and} \quad \begin{cases} \xi = \varepsilon\eta', \\ \eta = \varepsilon^{-1}\xi', \end{cases}$$

where ε is an arbitrary unit in Ω. The condition $(\alpha, \beta, \gamma) = (1)$ in Theorem 4, when $\alpha = \gamma = 0$, is satisfied when β is a unit in Ω and it is not difficult to verify that the theorem holds in this case too.

It should be noted that even if $(\alpha, \beta, \gamma) \neq (1)$ the values of π, ϱ, σ and τ in the theorem give integral automorphs but these may not be the only integral automorphs.

The lower signs in (9) give the indirect automorphs. Since the combination of two indirect automorphs gives a direct automorph all indirect automorphs are obtained from the combination of one particular indirect automorph with every one of the direct automorphs. We do not here discuss conditions for the existence of indirect automorphs.

Chapter II

DETERMINATION OF THE D-NUMBERS IN $\mathbf{K}(\sqrt{-1})$ FOR $D = 2, 3, 7, 11, 19, 43, 67$ AND 163

6. Some general properties of δ-numbers and δ-representations

In this chapter we are going to study D-numbers in $\mathbf{K}(\sqrt{-1})$ for some special rational integral values of D, but we start with some general remarks on δ-numbers in an algebraic field Ω.

Lemma 4. *The product of two δ-numbers in Ω is a δ-number in Ω.*

Proof. $(\xi^2 + \delta\eta^2)(\xi_1^2 + \delta\eta_1^2) = (\xi\xi_1 \pm \delta\eta\eta_1)^2 + \delta(\xi\eta_1 \mp \eta\xi_1)^2$.

An integer π in Ω is called a PRIME if the principal ideal (π) is a prime ideal in Ω. A prime that is a δ-number is called a δ-PRIME, and a unit in Ω that is a δ-number is called a δ-UNIT. If π is a prime in Ω not dividing 2 and if α is an integer in Ω not divisible by π we denote by $\left[\frac{\alpha}{\pi}\right]$ the usual *quadratic residue symbol*, i.e. $\left[\frac{\alpha}{\pi}\right] = 1$ if α is a quadratic residue modulo π and $\left[\frac{\alpha}{\pi}\right] = -1$ otherwise. In the rational field $\mathbf{K}(1)$ we shall use the symbol $\left(\frac{a}{p}\right)$.

Now let ω be a δ-number in Ω,

$$\omega = \alpha^2 + \delta\beta^2,$$

where α and β are integers in Ω. Suppose ω is divisible by a prime π not dividing 2δ. If π does not divide α, neither does it divide β and it follows that $\left[\frac{-\delta}{\pi}\right] = 1$. Thus if $\left[\frac{-\delta}{\pi}\right] = -1$ then π must divide α and hence also β. But then ω must be divisible by π^2 and ω/π^2 is also a δ-number in Ω. This suffices to prove the following two lemmata.

Lemma 5. *If ω is a δ-number in Ω and if π is a prime dividing ω such that $\left[\frac{-\delta}{\pi}\right] = -1$, then ω/π^2 is a δ-number in Ω.*

Lemma 6. *A necessary condition for a prime π not dividing 2δ to be a δ-number in Ω is* $\left[\frac{-\delta}{\pi}\right] = 1$.

Lemma 7. *If $\pi\omega$ is a δ-number in Ω and π is a δ-prime or a δ-unit in Ω then ω is a δ-number in Ω.*

Proof. Suppose $\pi\omega = \alpha^2 + \delta\beta^2$ and $\pi = \mu^2 + \delta\nu^2$ with integers α, β, μ and ν in Ω. Then

$$\pi^2\omega = (\alpha^2 + \delta\beta^2)(\mu^2 + \delta\nu^2) = (\alpha\mu \pm \delta\beta\nu)^2 + \delta(\alpha\nu \mp \beta\mu)^2 \tag{10}$$

gives a δ-representation of ω if π is a unit. If π is a prime then from

$$(\alpha\nu + \beta\mu)(\alpha\nu - \beta\mu) = \alpha^2\nu^2 - \beta^2\mu^2 = \pi(\omega\nu^2 - \beta^2)$$

it follows that for at least one sign $\alpha\nu \mp \beta\mu$ is divisible by π. For the corresponding sign then also $\alpha\mu \pm \delta\beta\nu$ is divisible by π, and (10) gives a δ-representation of ω.

7. Some lemmata for D-representations in $\mathbf{K}(\sqrt{-1})$

In the rest of this chapter we are going to study D-representations in the gaussian number field $\Omega = \mathbf{K}(\sqrt{-1})$ for some rational square-free integral values of D. It is sufficient to consider *positive* D, since $\xi^2 - D\eta^2 = \xi^2 + D(\eta i)^2$. We also want to restrict the values of D so that $\mathbf{K}(\sqrt{D})$ and $\mathbf{K}(\sqrt{-D})$ are *simple fields* (i.e. with class number 1). Then also $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$ is simple. These conditions are satisfied for

$$D = 2, 3, 7, 11, 19, 43, 67, 163 \tag{11}$$

and perhaps a ninth value of D. In the following D shall be assumed to have one of the values (11) unless stated otherwise, and for these values we shall completely determine the D-numbers in $\mathbf{K}(\sqrt{-1})$.

Unless stated otherwise Latin letters stand for rational integers (except $i = \sqrt{-1}$), while lower case Greek letters denote integers in the quadratic field $\mathbf{K}(\sqrt{-1})$. Capital Greek letters will be used for integers in the biquadratic field $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$. D-numbers in $\mathbf{K}(\sqrt{-1})$ will be referred to simply as *D-numbers*.

In the following sections we must treat four different cases:

1°. $D = 2$; 2°. $D = 3$; 3°. $D = 7$; 4°. $D = 11, 19, 43, 67$ and 163.

The differences are due to different residues of D modulo 8. Case 2° separates from case 4° because $\mathbf{K}(\sqrt{-3})$ contains a non-real root of unity.

In this section we give some general results.

From

$$(x+yi)^2 + D(u+vi)^2 = x^2 - y^2 + D(u^2 - v^2) + 2(xy + Duv)i$$

it is immediately clear that a necessary condition for an integer $\omega = a+bi$, with a and b rational integers, to be a D-number is that b is *even*. We shall also often make use of the fact that ω is a D-number if and only if $-\omega$ is a D-number.

If π is a prime not dividing 2 in $\mathbf{K}(\sqrt{-1})$ then it is of the form $\pm(a+2bi)$ or $\pm i(a+2bi)$ with rational integers a and b, a odd. Therefore, if π is a given such prime, then of the four associate primes $\pm\pi$ and $\pm\pi i$ at most two are D-numbers. Neglecting a unit factor we can always assume a prime π not dividing 2 to be of the form $a+2bi$ with a odd.

Lemma 8. *If Λ is an integer in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$ then $2\Lambda = a+bi+(c+di)\sqrt{-D}$ with rational integers a, b, c and d.*

Proof. See for instance Nagell [6], p. 8.

Lemma 9. *If D is a rational integer such that D is odd or $D \equiv 2 \pmod 4$ and if*

$$a^2 - b^2 + D(c^2 - d^2) \equiv 4 \pmod 8, \tag{12}$$

$$ab + Dcd \equiv 0 \pmod 4, \tag{13}$$

with rational integers a, b, c and d, then one of the following alternatives is valid:

1°. *a, b, c and d are all even.*

2°. *a and c are odd, $b \equiv d \equiv 0$ or $\equiv 2 \pmod 4$; or*
b and d are odd, $a \equiv c \equiv 0$ or $\equiv 2 \pmod 4$.
In this case $D \equiv 3 \pmod 8$.

3°. *a and d are odd, $b \equiv c \equiv 0$ or $\equiv 2 \pmod 4$; or*
b and c are odd, $a \equiv d \equiv 0$ or $\equiv 2 \pmod 4$.
In this case $D \equiv 5 \pmod 8$.

Proof. If $D \equiv 2 \pmod 4$ then from (13) it follows that ab is even. (12) implies that both a and b are even, and then (13) gives cd even. By (12) c and d are both even.

Now let D be odd. Then because of (12) a, b, c and d cannot all be odd. Neither can three of the numbers be even (odd) and the fourth odd (even). From (13) it then follows that neither ab nor cd can be odd. Investigation of the remaining cases ac odd, ad odd, bc odd and bd odd proves the lemma.

In order to determine the D-primes in $\mathbf{K}(\sqrt{-1})$ we shall use the factorization of prime ideals (π) in $\mathbf{K}(\sqrt{-1})$ into prime ideals in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$. A prime ideal (π) in $\mathbf{K}(\sqrt{-1})$ that does not divide $2D$ *factorizes into two different prime ideals* in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$ if $\left[\frac{-D}{\pi}\right] = 1$, and it *is still a prime ideal* in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$ if $\left[\frac{-D}{\pi}\right] = -1$.

The *primes* in $\mathbf{K}(\sqrt{-1})$ are

1°. $(1+i)\varepsilon$;

2°. $p\varepsilon$, where the rational prime p is congruent 3 modulo 4;

3°. $\pi\varepsilon$, where the rational prime $p = \pi\pi'$ is congruent 1 modulo 4. π can be written $\pi = a + 2bi$ (a and b rational) with odd a.

ε denotes a *unit* (± 1 or $\pm i$) in $\mathbf{K}(\sqrt{-1})$. This notation will be used in the following.

For the primes $(1+i)\varepsilon$ we immediately obtain the following lemma.

Lemma 10. *$(1+i)\varepsilon$ is not a D-prime for any unit ε in $\mathbf{K}(\sqrt{-1})$.*

The odd values of D that we are considering are rational primes congruent 3 modulo 4. Hence they are primes in $\mathbf{K}(\sqrt{-1})$, and the representation

$$D = 0^2 + D \cdot 1^2$$

gives the next lemma.

Lemma 11. *If D is a rational prime congruent 3 modulo 4, then $\pm D$ but not $\pm Di$ are D-primes in $\mathbf{K}(\sqrt{-1})$.*

Lemma 12. *Let p be a rational prime congruent 1 modulo 4, factorizing into $p = \pi\pi'$, with primes π and π' in $\mathbf{K}(\sqrt{-1})$, and such that $\left(\frac{-D}{p}\right) = -1$. Then $\pi\varepsilon$ is not a D-prime for any unit ε in $\mathbf{K}(\sqrt{-1})$.*

Proof. With the conditions in the lemma, $N(\pi\varepsilon) = p$ and hence $\left[\frac{-D}{\pi\varepsilon}\right] \equiv (-D)^{(p-1)/2} \pmod{\pi\varepsilon}$ (see for instance Hilbert [3], § 1). Thus $\left[\frac{-D}{\pi\varepsilon}\right] = -1$ and Lemma 6 completes the proof.

Lemma 13. *Let p be a rational prime congruent 3 modulo 4 and such that $\left(\frac{D}{p}\right) = 1$. Then $\pm p$ but not $\pm pi$ are D-primes in $\mathbf{K}(\sqrt{-1})$.*

Proof. Since $\left(\frac{D}{p}\right) = 1$, p factors in $\mathbf{K}(\sqrt{D})$, $ep = (u + v\sqrt{D})(u - v\sqrt{D})$ with $e = 1$ or $e = -1$. Our considered values of D are primes congruent 2 or 3 modulo 4, so that u and v are integers. Hence $ep = u^2 + D(vi)^2$ is a D-representation.

We shall also have to use a decomposition of the unit i (and $-i$) into two conjugate (relative to $\mathbf{K}(\sqrt{-1})$ factors in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$. Since $D \equiv 2$ or $3 \pmod 4$ the principal ideal (2) can be factorized into two equal prime ideal factors in $\mathbf{K}(\sqrt{D})$. Then for some unit η in $\mathbf{K}(\sqrt{D})$

$$2 = (s + t\sqrt{D})^2 \eta$$

with rational integers s and t. But then also

$$2 = (s - t\sqrt{D})^2 \eta',$$

where η' is the conjugate unit of η, such that $\eta\eta' = 1$. Hence

$$4 = (s^2 - Dt^2)^2 \eta\eta',$$

and

$$2 = \pm (s^2 - Dt^2) \tag{14}$$

for one of the signs. This gives the factorization

$$\pm i = \frac{(1+i)(s+t\sqrt{D})}{2} \cdot \frac{(1+i)(s-t\sqrt{D})}{2}$$

for one of the signs. The two factors are integers in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$. This gives the following lemma.

Lemma 14. *If an integer ω in $\mathbf{K}(\sqrt{-1})$ factorizes into two conjugate (relative to $\mathbf{K}(\sqrt{-1})$) integers in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$, then $-\omega$, ωi and $-\omega i$ do so too.*

From (14) and $2i=(1+i)^2$ immediately follows the next lemma.

Lemma 15. *± 2 and $\pm 2i$ are D-numbers.*

Lemma 16. *If $D\equiv 3 \pmod 8$ then $\pm(1+i)^n$ are D-numbers in $\mathbf{K}(\sqrt{-1})$ if and only if n is even $\geqslant 0$. $\pm i(1+i)^n$ are D-numbers if and only if n is even $\geqslant 2$.*

Proof. Suppose

$$\varepsilon(1+i)^n=\alpha^2+D\beta^2=(\alpha+\beta\sqrt{-D})(\alpha-\beta\sqrt{-D}),$$

where ε is equal to ± 1 or $\pm i$, n is a rational integer $\geqslant 0$ and α and β are integers in $\mathbf{K}(\sqrt{-1})$. Now $1+i$ is a prime in $\mathbf{K}(\sqrt{-1},\sqrt{-D})$ if $D\equiv 3 \pmod 8$ (see Hilbert [2], § 2). Hence

$$\alpha+\beta\sqrt{-D}=(1+i)^k\Gamma,$$

where Γ is a unit in $\mathbf{K}(\sqrt{-1},\sqrt{-D})$ and k is a rational integer $\geqslant 0$. If Γ' is the conjugate number of Γ relative to $\mathbf{K}(\sqrt{-1})$ then

$$\alpha-\beta\sqrt{-D}=(1+i)^k\Gamma'.$$

Hence $n=2k$ and $\Gamma\Gamma'=\varepsilon$.

If $\varepsilon=\pm 1$ the condition $n=2k\geqslant 0$ then is necessary, but it is immediately clear that it is also sufficient.

If $\varepsilon=\pm i$ then also $n=2k$ is necessary, but for $n=0$ there are no D-numbers. Now according to Lemma 15 the integers $\pm i(1+i)^2$ are D-numbers and consequently $\pm i(1+i)^n$ are D-numbers for all even $n\geqslant 2$ (cf. Lemma 4).

8. The case $D=2$

According to Lemmata 10, 12 and 13 we have to consider the two cases (i) $p\equiv 1 \pmod 4$ and $\left(\frac{2}{p}\right)=1$; and (ii) $p\equiv 3 \pmod 4$ and $\left(\frac{2}{p}\right)=-1$; in order to find all 2-primes. Here p denotes a rational prime.

(i) $\qquad p\equiv 1 \pmod 4$ and $\left(\frac{2}{p}\right)=1$, i.e. $p\equiv 1 \pmod 8$.

Then $p=\pi\pi'$ in $\mathbf{K}(\sqrt{-1})$ with the prime $\pi=a+2bi$ (a and b rational integers), a odd. $\left(\frac{2}{\pi}\right)=1$ and hence

$$\varepsilon\pi = \Pi\Pi'$$

with conjugate primes Π and Π' in $\mathbf{K}(\sqrt{-1}, \sqrt{-2})$, and by Lemma 14 we can assume $\varepsilon = 1$. Lemma 8 gives $2\Pi = x + yi + (u + vi)\sqrt{-2}$ with rational integers x, y, u and v. Then

$$x^2 - y^2 + 2(u^2 - v^2) = 4a \equiv 4 \pmod 8,$$

$$xy + 2uv = 4b \equiv 0 \pmod 4,$$

and owing to Lemma 9 x, y, u and v are all even. Hence π is a 2-prime in $\mathbf{K}(\sqrt{-1})$ with the representation

$$\pi = \left(\frac{x + yi}{2}\right)^2 + 2\left(\frac{u + vi}{2}\right)^2.$$

$\pm\pi = \pm(a + 2bi)$ *are 2-primes but not* $\pm\pi i$.

(ii) $\quad p \equiv 3 \pmod 4$ and $\left(\frac{2}{p}\right) = -1$, i.e. $p \equiv 3 \pmod 8$.

Then p is a prime in $\mathbf{K}(\sqrt{-1})$ but in $\mathbf{K}(\sqrt{-2})$ p has the decomposition

$$p = (u + v\sqrt{-2})(u - v\sqrt{-2}) = u^2 + 2v^2$$

with rational integers u and v.

$\pm p$ *are 2-primes but not* $\pm pi$.

The above results give the following conditions for a prime in $\mathbf{K}(\sqrt{-1})$ to be a 2-prime.

Theorem 6 A. *If π is a prime not dividing 2 in $\mathbf{K}(\sqrt{-1})$ then π is a 2-prime in $\mathbf{K}(\sqrt{-1})$ if and only if $\left[\frac{-2}{\pi}\right] = 1$ and $\pi = a + 2bi$ with rational integers a and b. $\pm(1 \pm i)$ are not 2-primes.*

Now let ω be an arbitrary integer in $\mathbf{K}(\sqrt{-1})$. It can be written as a product

$$\omega = \varepsilon\alpha\beta(1 + i)^n,$$

where ε is a unit (± 1 or $\pm i$), α is a product of 2-primes, β is a product of primes $\pi = c + 2di$ (c and d rational integers) for which $\left[\frac{-2}{\pi}\right] = -1$,

and n is a rational integer $\geqslant 0$. Here and in the following *a product is allowed to be empty*, i.e. α or β may be equal to 1.

Suppose ω is a 2-number. Then by Lemma 7 ω/α is a 2-number, and from Lemma 5 it follows that β must be a square and $\omega/\alpha\beta$ is also a 2-number. Hence $\varepsilon(1+i)^n$ must be a 2-number.

Lemma 17. *$\pm(1+i)^n$ are 2-numbers if and only if $n=0$ or $n\geqslant 2$. $\pm i(1+i)^n$ are 2-numbers if and only if $n\geqslant 2$.*

Proof. $(1+i)^n$ is a 2-number for any even $n\geqslant 0$. For $n=1$ it is not a 2-number, but it is a 2-number for $n=3$, because

$$(1+i)^3=(1+i)^2+2i^2.$$

Owing to Lemma 4 then $(1+i)^n$ is a 2-number for $n=0$ and $n\geqslant 2$.

$i(1+i)^n$ is not a 2-number for $n=0$ or $n=1$. But

$$i(1+i)^2=2i^2$$

and

$$i(1+i)^3=(1-i)^2+2i^2.$$

Hence $i(1+i)^n$ is a 2-number for $n\geqslant 2$.

Thus we obtain the necessary conditions for an integer in $\mathbf{K}(\sqrt{-1})$ to be a 2-number which we state in the following theorem. It is easy to see, using Lemma 4, that these conditions are also sufficient.

Theorem 6 B. *The integer*

$$\omega=\varepsilon\alpha\beta(1+i)^n$$

in $\mathbf{K}(\sqrt{-1})$, where $\varepsilon=\pm 1$ or $\pm i$, α is a product of 2-primes, β is a product of primes $\pi=c+2di$ (c and d rational integers) with $\left[\frac{-2}{\pi}\right]=-1$, and n is a non-negative rational integer, is a 2-number in $\mathbf{K}(\sqrt{-1})$ if and only if β is a square and

1°. *$n\geqslant 2$; or*

2°. *$n=0$ and $\varepsilon=\pm 1$.*

9. The case $D=3$

First we study the decomposition of rational primes p.

(i) $$p\equiv 1 \pmod 4 \text{ and } \left(\frac{3}{p}\right)=1, \text{ i.e. } p\equiv 1 \pmod{12}.$$

Then $p=\pi\pi'$ in $\mathbf{K}(\sqrt{-1})$ with the prime $\pi=a+2bi$ (a and b rational integers), a odd. $\left[\frac{-3}{\pi}\right]=1$ and hence

$$\varepsilon\pi=\Pi\Pi'$$

with conjugate primes Π and Π' in $\mathbf{K}(\sqrt{-1},\sqrt{-3})$ and by Lemma 14 we can assume $\varepsilon=1$. Lemma 8 gives $2\Pi=x+yi+(u+vi)\sqrt{-3}$ with rational integers x, y, u and v, and thus

$$x^2-y^2+3(u^2-v^2)=4a\equiv 4 \pmod 8$$
$$xy+3uv=4b\equiv 0 \pmod 4.$$

If x, y, u and v are not all even, then by Lemma 9 either xu is odd and $y\equiv v\equiv 0$ or $\equiv 2 \pmod 4$ or yv is odd and $x\equiv u\equiv 0$ or $\equiv 2 \pmod 4$. Now $\mathbf{K}(\sqrt{-1},\sqrt{-3})$ contains the roots of unity $\frac{1}{2}(1\pm\sqrt{-3})$, and $\pi=\Pi\Pi'=\Pi\Gamma\Pi'\Gamma'$ with $\Gamma=\frac{1}{2}(1+\sqrt{-3})$ or $\Gamma=\frac{1}{2}(1-\sqrt{-3})$ and Γ' the conjugate number of Γ relative to $\mathbf{K}(\sqrt{-1})$. Then

$$\Pi\Gamma=\tfrac{1}{2}[x+yi+(u+vi)\sqrt{-3}]\cdot\tfrac{1}{2}(1\pm\sqrt{-3})$$
$$=\tfrac{1}{4}[x_1+y_1i+(u_1+v_1i)\sqrt{-3}]$$

with $\qquad x_1=x\mp 3u,\quad y_1=y\mp 3v,\quad u_1=\pm x+u,\quad v_1=\pm y+v.$

Suppose xu is odd. Then we can choose the sign in $\Gamma=\frac{1}{2}(1\pm\sqrt{-3})$ so that $x_1\equiv 0 \pmod 4$, which also implies $u_1\equiv 0 \pmod 4$. Because the even integers y and v are congruent modulo 4 also $y_1\equiv v_1\equiv 0 \pmod 4$. If yv is odd it is also possible to choose the sign in Γ so that

$$x_1\equiv y_1\equiv u_1\equiv v_1\equiv 0 \pmod 4.$$

Then
$$\pi=\left(\frac{x_1+y_1i}{4}\right)^2+3\left(\frac{u_1+v_1i}{4}\right)^2$$

is a 3-representation of π in $\mathbf{K}(\sqrt{-1})$.

$\pm\pi=\pm(a+2bi)$ *are 3-primes but not* $\pm\pi i$.

(ii) $\qquad p\equiv 3 \pmod 4$ and $\left(\frac{3}{p}\right)=-1$, i.e. $p\equiv 7 \pmod{12}$.

Then p is a prime in $\mathbf{K}(\sqrt{-1})$. $\left(\frac{-3}{p}\right)=1$ gives

$$p = \tfrac{1}{2}(u + v\sqrt{-3}) \cdot \tfrac{1}{2}(u - v\sqrt{-3}) = \tfrac{1}{4}(u^2 + 3v^2)$$

with rational integers u and v of the same parity. If u and v are both even, p is a 3-prime. If u and v are both odd we multiply by $\Gamma\Gamma' = 1$, where $\Gamma = \tfrac{1}{2}(1 \pm \sqrt{-3})$ and $\Gamma' = \tfrac{1}{2}(1 \mp \sqrt{-3})$.

$$\tfrac{1}{2}(u + v\sqrt{-3}) \cdot \tfrac{1}{2}(1 \pm \sqrt{-3}) = \tfrac{1}{4}(u_1 + v_1\sqrt{-3}),$$

where
$$u_1 = u \mp 3v, \quad v_1 = v \pm u.$$

The sign can be chosen so that $u_1 \equiv v_1 \equiv 0 \pmod 4$, and hence p is a 3-prime.

$\pm p$ are 3-primes but not $\pm pi$.

Together with Lemmata 10, 11, 12 and 13 we obtain the following result.

Theorem 7 A. *If π is a prime not dividing 6 in $\mathbf{K}(\sqrt{-1})$ then π is a 3-prime in $\mathbf{K}(\sqrt{-1})$ if and only if $\left[\frac{-3}{\pi}\right] = 1$ and $\pi = a + 2bi$ with rational integers a and b. ± 3 are 3-primes but not $\pm 3i$ or $\pm(1 \pm i)$.*

We now want to find conditions for an arbitrary integer in $\mathbf{K}(\sqrt{-1})$ to be a 3-number. Any integer ω in $\mathbf{K}(\sqrt{-1})$ can be written

$$\omega = \varepsilon\alpha\beta(1 + i)^n,$$

where ε is a unit (± 1 or $\pm i$), α is a product of 3-primes, β is a product of primes $\pi = c + 2di$ (c and d rational integers) for which $\left[\frac{-3}{\pi}\right] = -1$, and n is a rational integer $\geqslant 0$.

Suppose ω is a 3-number. Then from Lemma 7 it follows that ω/α must be a 3-number. Owing to Lemma 5 the integer β must be a square and $\omega/\alpha\beta$ is also a 3-number. Hence $\varepsilon(1 + i)^n$ must be a 3-number. Then Lemma 16 completes the necessary conditions for an integer in $\mathbf{K}(\sqrt{-1})$ to be a 3-number, as stated in the following theorem. The sufficiency of the conditions easily follows from Lemma 4.

Theorem 7 B. *The integer*

$$\omega = \varepsilon\alpha\beta(1 + i)^n$$

in $\mathbf{K}(\sqrt{-1})$, where $\varepsilon = \pm 1$ or $\pm i$, α is a product of 3-primes, β is a

product of primes $\pi = c + 2di$ *(*c *and* d *rational integers) with* $\left[\frac{-3}{\pi}\right] = -1$, *and* n *is a non-negative rational integer, is a 3-number in* $\mathbf{K}(\sqrt{-1})$ *if and only if* β *is a square and*

1°. n *is even* $\geqslant 2$; *or*

2°. $n = 0$ *and* $\varepsilon = \pm 1$.

10. The case $D = 7$

First we study the decomposition of rational primes p.

(i) $$p \equiv 1 \pmod 4, \left(\frac{7}{p}\right) = 1, \text{ i.e. } p \equiv 1, 9, 25 \pmod{28}.$$

Then $p = \pi\pi'$ in $\mathbf{K}(\sqrt{-1})$ with the prime $\pi = a + 2bi$ (a and b rational integers), a odd. $\left[\frac{-7}{\pi}\right] = 1$ and hence

$$\varepsilon\pi = \Pi\Pi'$$

with conjugate primes Π and Π' in $\mathbf{K}(\sqrt{-1}, \sqrt{-7})$ and by Lemma 14 we can assume $\varepsilon = 1$. Lemmata 8 and 9 give $\Pi = x + yi + (u + vi)\sqrt{-7}$ with rational integers x, y, u and v and thus

$$\pi = (x + yi)^2 + 7(u + vi)^2$$

is a 7-representation of π in $\mathbf{K}(\sqrt{-1})$.

$\pm\pi = \pm(a + 2bi)$ *are 7-primes but not* $\pm\pi i$.

(ii) $$p \equiv 3 \pmod 4, \left(\frac{7}{p}\right) = -1, \text{ i.e. } p \equiv 11, 15, 23 \pmod{28}.$$

Then p is a prime in $\mathbf{K}(\sqrt{-1})$. $\left(\frac{-7}{p}\right) = 1$ gives

$$p = \tfrac{1}{2}(u + v\sqrt{-7}) \cdot \tfrac{1}{2}(u - v\sqrt{-7}) = \tfrac{1}{4}(u^2 + 7v^2)$$

with rational integers u and v of the same parity. But u and v cannot both be odd since p is odd. Hence $p = (u/2)^2 + 7(v/2)^2$ is a 7-representation of p.

$\pm p$ *are 7-primes but not* $\pm pi$.

The above results can be stated as follows.

Theorem 8 A. *If π is a prime not dividing 14 in $\mathbf{K}(\sqrt{-1})$ then π is a 7-prime in $\mathbf{K}(\sqrt{-1})$ if and only if $\left[\frac{-7}{\pi}\right]=1$ and $\pi=a+2bi$ with rational integers a and b. ± 7 are 7-primes but not $\pm 7i$ or $\pm(1\pm i)$.*

In the above theorem we have completely determined the 7-primes and we now turn to 7-numbers in general. Any integer ω in $\mathbf{K}(\sqrt{-1})$ can be written

$$\omega=\varepsilon\alpha\beta(1+i)^n,$$

where ε is a unit (± 1 or $\pm i$), α is a product of 7-primes, β is a product of primes $\pi=c+2di$ (c and d rational integers) for which $\left[\frac{-7}{\pi}\right]=-1$, and n is a rational integer $\geqslant 0$.

Suppose ω is a 7-number. Then it follows that β must be a square and $\varepsilon(1+i)^n$ must be a 7-number. Now we cannot use Lemma 16, but we can prove a similar result.

Lemma 18. *$\pm(1+i)^n$ are 7-numbers if and only if $n=0$ or $n=2$ or $n\geqslant 4$. $\pm i(1+i)^n$ are 7-numbers if and only if $n=2$ or $n\geqslant 4$.*

Proof. The prime ideal $(1+i)$ in $\mathbf{K}(\sqrt{-1})$ factorizes into two different prime ideals in $\mathbf{K}(\sqrt{-1},\sqrt{-7})$ (see Hilbert [2], § 2),

$$(1+i)=(\Lambda)(\Lambda').$$

We can choose

$$\Lambda=\tfrac{1}{2}[8-5i+(2+3i)\sqrt{-7}],\quad \Lambda'=\tfrac{1}{2}[8-5i-(2+3i)\sqrt{-7}].$$

Then
$$4(1+i)=(8-5i)^2+7(2+3i)^2, \tag{15}$$

i.e. $(1+i)^5$ is a 7-number in $\mathbf{K}(\sqrt{-1})$. Of course $(1+i)^n$ is a 7-number for every even $n\geqslant 0$, and hence owing to Lemma 4 $(1+i)^n$ is a 7-number for $n=0$, $n=2$ and $n\geqslant 4$. $1+i$ is not a 7-number and neither is $(1+i)^3$ as we shall now show.

Suppose

$$(\Lambda\Lambda')^3=(1+i)^3=\alpha^2+7\beta^2=(\alpha+\beta\sqrt{-7})(\alpha-\beta\sqrt{-7}),$$

where α and β are integers in $\mathbf{K}(\sqrt{-1})$. Then, with Γ and Γ' conjugate units in $\mathbf{K}(\sqrt{-1},\sqrt{-7})$,

$$\begin{cases}\alpha+\beta\sqrt{-7}=\Lambda^3\Gamma\\ \alpha-\beta\sqrt{-7}=\Lambda'^3\Gamma'\end{cases}\quad\text{or}\quad\begin{cases}\alpha+\beta\sqrt{-7}=\Lambda^2\Lambda'\Gamma\\ \alpha-\beta\sqrt{-7}=\Lambda\Lambda'^2\Gamma'.\end{cases}$$

Adding the equations gives $2\alpha = \Lambda^3\Gamma + \Lambda'^3\Gamma'$ or $2\alpha = (1+i)(\Lambda\Gamma + \Lambda'\Gamma')$. In the first case Λ^3 should be divisible by Λ' which is impossible, and also the second case is impossible since Λ is not divisible by Λ'. Hence the lemma is proved for $\pm(1+i)^n$.

From (15) and Lemma 14 it follows that $\pm i(1+i)^5$ are 7-numbers in $\mathbf{K}(\sqrt{-1})$. Also $\pm(1+i)^2 = \mp 2$ are 7-numbers. Hence $\pm i(1+i)^n$ are 7-numbers for $n=2$ and $n \geqslant 4$. For $n=0$ and $n=1$ the integers $\pm i(1+i)^n$ are not 7-numbers and neither for $n=3$ by the same argument as used above for $\pm(1+i)^3$. This completes the proof of the lemma.

We are now able to give conditions for an arbitrary integer in $\mathbf{K}(\sqrt{-1})$ to be a 7-number.

Theorem 8 B. *The integer*

$$\omega = \varepsilon\alpha\beta(1+i)^n$$

in $\mathbf{K}(\sqrt{-1})$, *where* $\varepsilon = \pm 1$ *or* $\pm i$, α *is a product of 7-primes,* β *is a product of primes* $\pi = c + 2di$ (*c and d rational integers*) *with* $\left[\frac{-7}{\pi}\right] = -1$, *and* n *is a non-negative rational integer, is a 7-number in* $\mathbf{K}(\sqrt{-1})$ *if and only if* β *is a square and*

1°. $n=2$ *or* $n \geqslant 4$; *or*
2°. $n=0$ *and* $\varepsilon = \pm 1$.

11. The case $D = 11, 19, 43, 67$ or 163

For the case when $D = 11$, 19, 43, 67 or 163 we need some more lemmata. In this section we will use D to denote one of these values.

Lemma 19. *In every D-representation of the number* 4 *in* $\mathbf{K}(\sqrt{-1})$, $4 = \alpha^2 + D\beta^2$, α *and* β *are divisible by* 2.

Proof. If $4 = \alpha^2 + D\beta^2$ with integers α and β in $\mathbf{K}(\sqrt{-1})$, then

$$\Gamma = \tfrac{1}{2}(\alpha + \beta\sqrt{-D}) \quad \text{and} \quad \Gamma' = \tfrac{1}{2}(\alpha - \beta\sqrt{-D})$$

must be units in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$. With $\alpha = x + yi$ and $\beta = u + vi$ (x, y, u and v rational integers) we obtain

$$\Gamma = \tfrac{1}{2}[x+yi+(u+vi)\sqrt{-D}], \quad \Gamma' = \tfrac{1}{2}[x+yi-(u+vi)\sqrt{-D}],$$
$$\Gamma'' = \tfrac{1}{2}[x-yi+(u-vi)\sqrt{-D}], \quad \Gamma''' = \tfrac{1}{2}[x-yi-(u-vi)\sqrt{-D}].$$

$\Gamma\Gamma'$ is equal to 1 and $\Gamma\Gamma''$ is a unit in $\mathbf{K}(\sqrt{-D})$. For the values of D under consideration the only units in $\mathbf{K}(\sqrt{-D})$ are 1 and -1.

First suppose $\Gamma\Gamma'' = 1$. Then

$$\begin{cases} x^2 - y^2 + D(u^2 - v^2) = 4, \\ x^2 + y^2 - D(u^2 + v^2) = 4. \end{cases}$$

From this it follows that $y^2 - Du^2 = 0$ and hence $y = u = 0$. $x^2 - Dv^2 = 4$ is impossible modulo 8 if x and y are both odd. Hence x and v are both even and $\alpha = x$ and $\beta = vi$ are both divisible by 2.

If $\Gamma\Gamma'' = -1$ in the same manner it follows that $x = v = 0$, y and u even. Hence α and β are divisible by 2.

Lemma 20. *If π is a D-prime in $\mathbf{K}(\sqrt{-1})$ and if $4\pi = \alpha^2 + D\beta^2$ with integers α and β in $\mathbf{K}(\sqrt{-1})$, then α and β are both divisible by 2.*

Proof. Suppose

$$4\pi = \alpha^2 + D\beta^2 \quad \text{and} \quad \pi = \gamma^2 + D\delta^2$$

with integers α, β, γ and δ in $\mathbf{K}(\sqrt{-1})$. Then

$$4 = \frac{(\alpha^2 + D\beta^2)(\gamma^2 + D\delta^2)}{\pi^2} = \left(\frac{\alpha\gamma \pm D\beta\delta}{\pi}\right)^2 + D\left(\frac{\alpha\delta \mp \beta\gamma}{\pi}\right)^2.$$

According to the proof of Lemma 7 this is a D-representation of 4 for either the upper or the lower signs. For suitable choice of signs then Lemma 19 implies $\alpha\gamma \pm D\beta\delta = 2\pi\mu$ and $\alpha\delta \mp \beta\gamma = 2\pi\nu$ with integers μ and ν in $\mathbf{K}(\sqrt{-1})$. This gives

$$\alpha = 2(\mu\gamma + D\nu\delta) \quad \text{and} \quad \pm\beta = 2(\mu\delta - \nu\gamma).$$

We are now able to give conditions for D-primes in $\mathbf{K}(\sqrt{-1})$. Let p be a rational prime.

(i) $$p \equiv 1 \pmod 4 \quad \text{and} \quad \left(\frac{D}{p}\right) = 1.$$

Then $p = \pi\pi'$ in $\mathbf{K}(\sqrt{-1})$ with the prime $\pi = a + 2bi$ (a and b rational integers), and

$$\pi = \Pi\Pi'$$

with Π and Π' conjugate (relative to $\mathbf{K}(\sqrt{-1})$) primes in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$. If $2\prod = x + yi + (u + vi)\sqrt{-D}$ with x, y, u and v rational integers then

$$4\pi = (x + yi)^2 + D(u + vi)^2.$$

By Lemma 20 the prime π *is a D-prime if and only if* x, y, u *and* v *are all even.*

(ii) $$p \equiv 3 \pmod 4 \quad \text{and} \quad \left(\frac{D}{p}\right) = -1.$$

Then $$p = \tfrac{1}{2}(u + v\sqrt{-D}) \cdot \tfrac{1}{2}(u - v\sqrt{-D}) = \tfrac{1}{4}(u^2 + Dv^2)$$

with rational integers u and v of the same parity. By Lemma 20 p *is a D-prime if and only if* u *and* v *are both even.*

With Lemmata 10, 11, 12 and 13 this gives the following characterization of the D-primes in $\mathbf{K}(\sqrt{-1})$.

Theorem 9 A. *The following primes in* $\mathbf{K}(\sqrt{-1})$ *and no others are D-primes in* $\mathbf{K}(\sqrt{-1})$ *for* $D = 11$, 19, 43, 67 *or* 163.

1°. $\pm p$, *where* p *is a rational prime* $\equiv 3 \pmod 4$ *and* $\left(\frac{D}{p}\right) = 1$.

2°. $\pm p$, *where* p *is a rational prime* $\equiv 3 \pmod 4$ *and* $\left(\frac{D}{p}\right) = -1$ *and* $p = u^2 + Dv^2$ *with rational integers* u *and* v.

3°. $\pi = a + 2bi$ (a *and* b *rational integers*), *where* $a^2 + 4b^2 = p$ *is a rational prime* $\equiv 1 \pmod 4$ *and* $\left(\frac{D}{p}\right) = 1$ *and* $a + 2bi = x^2 - y^2 + D(u^2 - v^2) + 2i(xu + Duv)$ *with rational integers* x, y, u *and* v.

4°. $\pm D$.

In order to determine conditions for arbitrary integers in $\mathbf{K}(\sqrt{-1})$ to be D-numbers, we must pay special attention to those primes $\pi = a + 2bi$ (a and b rational integers) in $\mathbf{K}(\sqrt{-1})$ for which $\left[\frac{-D}{\pi}\right] = 1$ but which are not D-primes. These primes will be called D-EXCEPTIONAL PRIMES in $\mathbf{K}(\sqrt{-1})$. As was shown in the proof of Theorem 9 A the D-exceptional primes are

1°. $\pi = a + 2bi$, *where* $a^2 + 4b^2 = p$ *is a rational prime* $\equiv 1 \pmod 4$ *with* $\left(\frac{D}{p}\right) = 1$ *and such that* $4\pi = (x + yi)^2 + D(u + vi)^2$ *with* x, y, u *and* v *not all even;*

2°. $\pm p$, *where* p *is a rational prime* $\equiv 3 \pmod 4$ *with* $\left(\frac{D}{p}\right) = -1$ *and such that* $4p = u^2 + Dv^2$ *with odd* u *and* v.

Lemma 21. *Let* $\omega = a + 2bi$ *and* $\omega_1 = a_1 + 2b_1 i$ *be integers in* $\mathbf{K}(\sqrt{-1})$ *with* a, b, a_1 *and* b_1 *rational integers,* a *and* a_1 *odd. Suppose* 4ω *and* $4\omega_1$ *have D-representations*

$$4\omega = \alpha^2 + D\beta^2 \quad \text{and} \quad 4\omega_1 = \alpha_1^2 + D\beta_1^2$$

such that none of the integers α, β, α_1 *and* β_1 *is divisible by* 2.

Then $\omega\omega_1$ *is a D-number. There is also a D-representation of* $4\omega\omega_1$,

$$4\omega\omega_1 = \mu^2 + D\nu^2,$$

with μ *and* ν *not divisible by* 2.

Proof. With the notations in the lemma we put

$$\alpha = x + yi, \quad \beta = u + vi, \quad \alpha_1 = x_1 + y_1 i, \quad \beta_1 = u_1 + v_1 i$$

with rational integers x, y, u, v, x_1, y_1, u_1 and v_1. Since none of the integers α, β, α_1 and β_1 is divisible by 2 we can according to Lemma 9 assume (possibly after multiplying ω or ω_1 by -1)

$$\begin{cases} x,\ u,\ x_1 \text{ and } u_1 \text{ are odd,} \\ y \equiv v \equiv 0 \text{ or } \equiv 2 \pmod 4, \\ y_1 \equiv v_1 \equiv 0 \text{ or } \equiv 2 \pmod 4. \end{cases}$$

We now consider the D-representations

$$16\omega\omega_1 = (\alpha\alpha_1 \pm D\beta\beta_1)^2 + D(\alpha\beta_1 \mp \beta\alpha_1)^2 \tag{16}$$

for the upper signs and for the lower signs.

$$\alpha\beta_1 \mp \beta\alpha_1 = xu_1 - yv_1 \mp (ux_1 - vy_1) + [xv_1 + yu_1 \mp (uy_1 + vx_1)]\, i.$$

Now $-yv_1 \pm vy_1 \equiv 0 \pmod 4$ and further $xv_1 \mp uy_1 \equiv yu_1 \mp vx_1 \equiv 0 \pmod 4$ for any choice of the sign. We can choose the sign such that $xu_1 \mp ux_1 \equiv 0 \pmod 4$. For this choice of sign $\alpha\beta_1 \mp \beta\alpha_1$ is divisible by 4 and then also $\alpha\alpha_1 \pm D\beta\beta_1$ is divisible by 4 for the corresponding sign. Hence (16) gives a D-representation of $\omega\omega_1$.

For the other choice of sign we obtain $xu_1 \mp ux_1 \equiv 2 \pmod 4$ which implies that $\alpha\beta_1 \mp \beta\alpha_1$ is divisible by 2 but not by 4 and then also

$\alpha\alpha_1 \pm D\beta\beta_1$ is divisible by 2 but not by 4 for the corresponding sign. Hence for this choice of signs (16) gives a D-representation of $4\omega\omega_1$ of the form $\mu^2 + D\nu^2$ with μ and ν not divisible by 2. This completes the proof of the lemma.

Lemma 22. *The product of k D-exceptional primes is a D-number if $k \geqslant 2$.*

Proof. If π and π_1 are D-exceptional primes they satisfy the conditions in Lemma 21 with $\pi = \omega$ and $\pi_1 = \omega_1$. Hence the product of two D-exceptional primes is a D-number. But according to Lemma 21 there is also a D-representation of $4\pi\pi_1$,

$$4\pi\pi_1 = \alpha_2^2 + D\beta_2^2,$$

with α_2 and β_2 not divisible by 2. And $\pi\pi_1$ is also of the form $a_2 + 2b_2 i$ (a_2 and b_2 rational integers) with a_2 odd. Hence we can apply Lemma 21 again to show that $\pi\pi_1\pi_2$ is a D-number, if π_2 is a D-exceptional prime. Induction on k proves Lemma 22.

We now want to investigate under what conditions $\varepsilon\gamma(1+i)^n$ is a D-number, where ε is a unit (± 1 or $\pm i$), γ a product of $k(\geqslant 1)$ D-exceptional primes and $n \geqslant 0$. Suppose

$$\varepsilon\gamma(1+i)^n = \alpha^2 + D\beta^2 = (\alpha + \beta\sqrt{-D})\,(\alpha - \beta\sqrt{-D})$$

with integers α and β in $\mathbf{K}(\sqrt{-1})$. Since $D \equiv 3 \pmod 8$ the ideal $(1+i)$ is a prime ideal in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$. Hence

$$\alpha + \beta\sqrt{-D} = (1+i)^t \cdot \tfrac{1}{2}(\xi + \eta\sqrt{-D})$$

for some rational integer $t \geqslant 0$, where $\frac{1}{2}(\xi + \eta\sqrt{-D})$ is an integer prime to $1+i$ in $\mathbf{K}(\sqrt{-1}, \sqrt{-D})$ with ξ and η integers in $\mathbf{K}(\sqrt{-1})$. Then

$$\alpha - \beta\sqrt{-D} = (1+i)^t \cdot \tfrac{1}{2}(\xi - \eta\sqrt{-D}),$$

where $\frac{1}{2}(\xi - \eta\sqrt{-D})$ is also prime to $1+i$. Hence

$$n = 2t \tag{17}$$

and

$$\varepsilon\gamma = \tfrac{1}{4}(\xi^2 + D\eta^2) \text{ with integers } \xi \text{ and } \eta \text{ in } \mathbf{K}(\sqrt{-1}). \tag{18}$$

It is also necessary that the numbers

$\frac{1}{2}(1+i)^t\xi$ and $\frac{1}{2}(1+i)^t\eta$ are integers in $\mathbf{K}(\sqrt{-1})$. (19)

Apparently the conditions (17), (18) and (19) are also sufficient for $\varepsilon\gamma(1+i)^n$ to be a D-number.

The condition (19) is satisfied as soon as $t \geqslant 2$ and ξ and η are integers, and (18) always holds. If γ is a D-number (i.e. if $k \geqslant 2$) and if $\varepsilon = \pm 1$, then (18) holds with ξ and η divisible by 2 and hence (19) is satisfied even for $t=0$ and $t=1$. If $t=0$ and $\varepsilon = \pm i$ then $\varepsilon\gamma(1+i)^n$ is not a D-number. If $t=0$ and $\varepsilon = \pm 1$ and if γ is a D-exceptional prime ($k=1$), then $\varepsilon\gamma(1+i)^n$ is not a D-number. The remaining cases to be considered are

$$\pm i\gamma(1+i)^2 = \mp 2\gamma \text{ when } k \geqslant 2, \text{ and}$$

$$\varepsilon\pi(1+i)^2 \text{ with } \pi \text{ a } D\text{-exceptional prime.}$$

According to Lemmata 4 and 15 the integer 2γ is a D-number if $k \geqslant 2$. Then suppose π is a D-exceptional prime and suppose

$$(1+i)^2\pi = (x+yi)^2 + D(u+vi)^2,$$

with rational integers x, y, u and v. Then

$$-4\pi = (1+i)^4\pi = (x_1+y_1i)^2 + D(u_1+v_1i)^2,$$

with $x_1 = x-y$ and $y_1 = x+y$ of the same parity. But this is in contradiction to Lemma 9, since π is not a D-number.

Finally, suppose

$$2\pi = (x+yi)^2 + D(u+vi)^2$$

with rational integers x, y, u and v. Since πi is not a D-number neither $x+yi$ nor $u+vi$ is divisible by $1+i$. Hence x and y are not of the same parity, neither are u and v. Now

$$i = \tfrac{1}{2}(-1+i)(s+t\sqrt{D}) \cdot \tfrac{1}{2}(-1+i)(s-t\sqrt{D})$$

where $s^2 - Dt^2 = -2$ (cf. Lemma 14). Then

$$2\pi i = (x_1+y_1i)^2 + D(u_1+v_1i)^2 \tag{20}$$

with $x_1 = -\frac{1}{2}[s(x+y) + Dt(u-v)]$ and similar values for y_1, u_1 and v_1, all of which are integers because s and t are both odd. Hence (20) should give a D-representation of $2\pi i$ but this has just been shown to be impossible. The conclusion is that 2π is not a D-number.

Lemma 23. *The integer*

$$\varepsilon\gamma(1+i)^n,$$

where ε *is a unit,* γ *a product of* $k(\geqslant 1)$ *D-exceptional primes and* $n \geqslant 0$, *is a D-number in* $\mathbf{K}(\sqrt{-1})$ *if and only if*

1°. n *is even* $\geqslant 4$; *or*

2°. $n=2$ *and* $k \geqslant 2$; *or*

3°. $n=0$ *and* $k \geqslant 2$ *and* $\varepsilon = \pm 1$.

We are now in a position to prove the main result about D-numbers for $D=11$, 19, 43, 67 and 163. Any integer ω in $\mathbf{K}(\sqrt{-1})$ can be written

$$\omega = \varepsilon\alpha\beta\gamma(1+i)^n,$$

where ε is a unit, α is a product of D-primes, β is a product of primes $\pi = c+2di$ (c and d rational integers) for which $\left[\frac{-D}{\pi}\right] = -1$, γ is a product of k D-exceptional primes and n is a non-negative rational integer.

Suppose ω is a D-number. Then β must be a square and $\varepsilon\gamma(1+i)^n$ must be a D-number. Lemmata 16 and 23 then give the necessary conditions for ω to be a D-prime as stated in the following theorem, and it is clear that these conditions are sufficient.

Theorem 9 B. *The integer*

$$\omega = \varepsilon\alpha\beta\gamma(1+i)^n$$

in $\mathbf{K}(\sqrt{-1})$, *where* $\varepsilon = \pm 1$ *or* $\pm i$, α *is a product of D-primes,* β *is a product of primes* $\pi = c+2di$ (c *and* d *rational integers*) *with* $\left[\frac{-D}{\pi}\right] = -1$, γ *is a product of* $k(\geqslant 0)$ *D-exceptional primes and n is a non-negative rational integer, is a D-number in* $\mathbf{K}(\sqrt{-1})$ ($D=11$, 19, 43, 67 *or* 163) *if and only if* β *is a square and n is even such that*

1°. $n \geqslant 4$; *or*

2°. $n=2$ *and* $k=0$ *or* $k \geqslant 2$; *or*

3°. $n=0$, $\varepsilon = \pm 1$ *and* $k=0$ *or* $k \geqslant 2$.

12. Remark on a result by Nagell

In his paper [6] Nagell determines the 1-numbers in certain quadratic fields. Theorem 14 in [6] stating conditions for an integer to be a

1-number in $\mathbf{K}(\sqrt{q})$, for $q=11$, 19, 43, 67 or 163, is in need of a correction. In fact, in the proof use is made of a lemma (Theorem 5 in [6]), which does not hold in all cases. The error in the proof of this lemma depends upon a choice of sign which is not justified. We get a counter example by putting $\Omega=\mathbf{K}(\sqrt{11})$, $\pi=3$, $\pi_1=23$, $\eta=4$ and $\alpha=207$. The conditions in the lemma are satisfied with $f=1$, $g=\sqrt{11}$, $f_1=9$ and $g_1=\sqrt{11}$, but $\alpha/\pi\pi_1=3$ is not a 1-number in $\mathbf{K}(\sqrt{11})$.

We want to restate Theorem 14 in [6] and give a new proof of that part where the lemma (Theorem 5 in [6]) was used.

In this section q will be used to denote one of the values 11, 19, 43, 67 and 163. Let *the fundamental unit* in $\mathbf{K}(\sqrt{q})$ be $\varepsilon_1=x_1+y_1\sqrt{q}$ with x_1 and y_1 positive rational integers. According to Lemma 16 in [6] x_1 is even and y_1 odd.

Let f and g be the least solutions of the equation $f^2-qg^2=-2$ in positive rational integers (f and g are both odd). Then ([6], p. 41)

$$2=(f+g\sqrt{q})^2\varepsilon_1{}^1.$$

Any prime π not dividing 2 is of the form $(a+2b\sqrt{q})\varepsilon$ with a and b rational integers, a odd, and ε a unit in $\mathbf{K}(\sqrt{q})$.

What Nagell calls an *A-number* is in our terminology a 1-*number*, and we use the term 1-*exceptional prime* for Nagell's *B-prime*, i.e. a prime $\pi=a+2b\sqrt{q}$ (a and b rational integers) in $\mathbf{K}(\sqrt{q})$ such that $\left[\frac{-1}{\pi}\right]=1$ in $\mathbf{K}(\sqrt{q})$ but which is not a 1-number in $\mathbf{K}(\sqrt{q})$. 4π is then a 1-number in $\mathbf{K}(\sqrt{q})$.

An arbitrary integer ω in $\mathbf{K}(\sqrt{q})$ can be written

$$\omega=\varepsilon_1^m\alpha\beta\gamma(f+g\sqrt{q})^n,$$

where α is a product of 1-primes, β is a product of primes π for which $\left[\frac{-1}{\pi}\right]=-1$, γ is a product of $k(\geqslant 0)$ 1-exceptional primes, m is a rational integer and n is a rational integer $\geqslant 0$.

If ω is a 1-number in $\mathbf{K}(\sqrt{q})$ and ω is divisible by a prime π for which $\left[\frac{-1}{\pi}\right]=-1$ then ω must be divisible by π^2 (Lemma 5). Hence $\beta\varepsilon$ must be a square for some unit ε and we can assume $\varepsilon=1$. Then

$$\varepsilon_1^m \gamma (f + g\sqrt{q})^n$$

has to be a 1-number in $\mathbf{K}(\sqrt{q})$.

For $k = 0$ we can use Lemma 19 in [6]:

Lemma 24. *The number $\varepsilon_1^m (f + g\sqrt{q})^n$ is a 1-number in $\mathbf{K}(\sqrt{q})$ if and only if n is even such that*

1°. $n \geqslant 2$; *or*

2°. $n = 0$ *and* m *even.*

For $k = 1$ we use Lemma 26 in [6]:

Lemma 25. *If π is a 1-exceptional prime in $\mathbf{K}(\sqrt{q})$ then $\varepsilon_1^m \pi (f + g\sqrt{q})^n$ is a 1-number in $\mathbf{K}(\sqrt{q})$ if and only if n is even $\geqslant 4$.*

For $k \geqslant 2$ we need the following lemmata.

Lemma 26. *Let $\omega = a + 2b\sqrt{q}$ and $\omega_1 = a_1 + 2b_1\sqrt{q}$ be integers in $\mathbf{K}(\sqrt{q})$ with a, b, a_1 and b_1 rational integers, a and a_1 odd. Suppose 4ω and $4\omega_1$ have 1-representations*

$$4\omega = \alpha^2 + \beta^2 \quad \text{and} \quad 4\omega_1 = \alpha_1^2 + \beta_1^2$$

in $\mathbf{K}(\sqrt{q})$ such that none of the integers α, β, α_1 and β_1 is divisible by 2.

Then $\omega\omega_1$ is a 1-number in $\mathbf{K}(\sqrt{q})$. There is also a 1-representation of $4\omega\omega_1$ in $\mathbf{K}(\sqrt{q})$,

$$4\omega\omega_1 = \mu^2 + \nu^2,$$

with μ and ν not divisible by 2.

Proof. Put

$$\alpha = x + y\sqrt{q}, \quad \beta = u + v\sqrt{q}, \quad \alpha_1 = x_1 + y_1\sqrt{q}, \quad \beta_1 = u_1 + v_1\sqrt{q}$$

with rational integers x, y, u, v, x_1, y_1, u_1 and v_1. From $4(a + 2b\sqrt{q}) = 4\omega = \alpha^2 + \beta^2$ it follows that

$$\begin{cases} x^2 + u^2 + q(y^2 + v^2) = 4a \equiv 4 \pmod 8, \\ xu + uv = 4b \equiv 0 \pmod 4. \end{cases}$$

This is possible in the following cases ([6], p. 45–46):

1°. x, y, u and v are all even;

2°. x and v are odd, $y \equiv u \equiv 0$ or $\equiv 2 \pmod 4$;

3°. y and u are odd, $x \equiv v \equiv 0$ or $\equiv 2 \pmod 4$.

Now according to the conditions in the lemma case 1° cannot occur. Hence we can always assume case 2° to hold (possibly after interchanging α and β). Similar conditions hold for ω_1 so we can always assume

$$\begin{cases} x,\ v,\ x_1 \text{ and } v_1 \text{ are odd,} \\ y \equiv u \equiv 0 \text{ or } \equiv 2 \pmod 4, \\ y_1 \equiv u_1 \equiv 0 \text{ or } \equiv 2 \pmod 4. \end{cases}$$

We now consider the 1-representations

$$16\omega\omega_1 = (\alpha\alpha_1 \pm \beta\beta_1)^2 + (\alpha\beta_1 \mp \beta\alpha_1)^2 \tag{21}$$

for the upper signs and for the lower signs. We obtain

$$\alpha\alpha_1 \pm \beta\beta_1 = xx_1 + qyy_1 \pm (uu_1 + qvv_1) + [xy_1 + yx_1 \pm (uv_1 + vu_1)]\sqrt{q}.$$

Now $qyy_1 \pm uu_1 \equiv 0 \pmod 4$ and $xy_1 \pm vu_1 \equiv yx_1 \pm uv_1 \equiv 0 \pmod 4$ for any sign. We can choose the sign such that $xx_1 \pm qvv_1$ is divisible by 4. Then $\alpha\alpha_1 \pm \beta\beta_1$ is divisible by 4 and also $\alpha\beta_1 \mp \beta\alpha_1$ is divisible by 4 for the corresponding sign. Hence (21) gives a 1-representation of $\omega\omega_1$ in $\mathbf{K}(\sqrt{q})$ (cf. Lemma 22 in [6]).

For the other choice of sign we obtain $xx_1 \pm qvv_1 \equiv 2 \pmod 4$ which implies that $\alpha\alpha_1 \pm \beta\beta_1$ is divisible by 2 but not by 4 and then also $\alpha\beta_1 \mp \beta\alpha_1$ is divisible by 2 but not by 4 for the corresponding sign. Hence for this choice of signs (21) gives a 1-representation

$$4\omega\omega_1 = \mu^2 + \nu^2$$

with μ and ν not divisible by 2. This completes the proof of the lemma.

Lemma 27. *The product of k 1-exceptional primes in $\mathbf{K}(\sqrt{q})$ is a 1-number in $\mathbf{K}(\sqrt{q})$ if $k \geqslant 2$.*

Proof. If π and π_1 are 1-exceptional primes in $\mathbf{K}(\sqrt{q})$ they satisfy the conditions in Lemma 26 with $\pi = \omega$ and $\pi_1 = \omega_1$. Hence the product $\pi\pi_1$ is a 1-number in $\mathbf{K}(\sqrt{q})$. $\pi\pi_1$ is also of the form $a_2 + 2b_2\sqrt{q}$ (a_2 and b_2 rational integers) with a_2 odd and by Lemma 26 there is a 1-representation $4\pi\pi_1 = \alpha_2^2 + \beta_2^2$ with α_2 and β_2 not divisible by 2. Hence we can apply Lemma 26 again to show that $\pi\pi_1\pi_2$ is a 1-number in $\mathbf{K}(\sqrt{q})$, if π_2 is a 1-exceptional prime in $\mathbf{K}(\sqrt{q})$. Induction on k proves the lemma.

We can now find conditions for an integer

$$\omega = \varepsilon_1^m \gamma (f + g\sqrt{q})^n$$

in $\mathbf{K}(\sqrt{-1})$, where γ is a product of $k(\geqslant 2)$ 1-exceptional primes in $\mathbf{K}(\sqrt{q})$, to be a 1-number in $\mathbf{K}(\sqrt{q})$.

Suppose

$$\omega = \varepsilon_1^m \gamma (f + g\sqrt{q})^n = \alpha^2 + \beta^2 = (\alpha + \beta i)(\alpha - \beta i)$$

with integers α and β in $\mathbf{K}(\sqrt{q})$. The integer $f + g\sqrt{q}$ is a prime in $\mathbf{K}(\sqrt{q}, \sqrt{-1})$ and as in the proof of Lemma 23 we obtain the necessary conditions

$$n \text{ is even}, \quad n = 2t.$$

$$\varepsilon_1^m \gamma = \tfrac{1}{4}(\xi^2 + \eta^2) \text{ with integers } \xi \text{ and } \eta \text{ in } \mathbf{K}(\sqrt{q}), \tag{22}$$

and

$$\tfrac{1}{2}(f + g\sqrt{q})^t \xi \text{ and } \tfrac{1}{2}(f + g\sqrt{q})^t \eta \text{ are integers in } \mathbf{K}(\sqrt{q}). \tag{23}$$

These three conditions are apparently also sufficient, since we then obtain a 1-representation (α, β) of ω with $\alpha = \tfrac{1}{2}(f + g\sqrt{q})^t \xi$ and $\beta = \tfrac{1}{2}(f + g\sqrt{q})^t \eta$.

(22) holds for any m (cf. Nagell [6], p. 44–45). If m is even (22) holds with ξ and η divisible by 2 (since γ is a 1-number) and then (23) holds for any t. If $t > 2$ then (23) always holds. The remaining cases are m odd with $n = 0$ or $n = 2$.

In [6], p. 41, it is shown that $\varepsilon_1 (f + g\sqrt{q})^2$ is a 1-number. Hence $\varepsilon_1^m \gamma (f + g\sqrt{q})^2$ is a 1-number also for odd m. $\varepsilon_1^m \gamma$ with m odd is not a 1-number since it is of the form $2a + b\sqrt{q}$ with b odd.

We have then proved the following result:

Lemma 28. *The integer*

$$\varepsilon_1^m \gamma (f + g\sqrt{q})^n,$$

where γ is a product of $k(\geqslant 2)$ 1-exceptional primes in $\mathbf{K}(\sqrt{q})$, is a 1-number in $\mathbf{K}(\sqrt{q})$ if and only if

1°. *n is even $\geqslant 2$; or*

2°. *$n = 0$ and m even.*

Using Lemmata 24, 25 and 28 we can now give the correct form of Theorem 14 in [6] (cf. [6], p. 50–51).

Theorem 10. *The integer ω in $\mathbf{K}(\sqrt{q})$ is a 1-number in $\mathbf{K}(\sqrt{q})$ if and only if*

$$\omega = \varepsilon_1^m \alpha\beta^2\gamma(f + g\sqrt{q})^n,$$

where $\varepsilon_1 = x_1 + y_1\sqrt{q}$ *is the fundamental unit in* $\mathbf{K}(\sqrt{q})$ *with positive rational integers* x_1 *and* y_1, α *is a product of 1-primes,* β *is a product of primes* π *with* $\left[\frac{-1}{\pi}\right] = -1$, γ *is a product of* $k(\geqslant 0)$ *1-exceptional primes,* f *and* g *are the least solutions of the equation* $f^2 - gq^2 = 2$ *in positive rational integers,* m *is a rational integer and* n *is an even rational integer, such that*

1°. $n \geqslant 4$; *or*

2°. $n = 2$ *and* $k = 0$ *or* $k \geqslant 2$; *or*

3°. $n = 0$, m *even and* $k = 0$ *or* $k \geqslant 2$.

13. Remark on (α, β, γ)-numbers in $\mathbf{K}(\sqrt{-1})$ with $4\alpha\gamma - \beta^2 = D$

We assume in this section $\alpha \neq 0$. It then follows

$$\alpha\xi^2 + \beta\xi\eta + \gamma\eta^2 = (4\alpha)^{-1}[(2\alpha\xi + \beta\eta)^2 + \delta\eta^2],$$

where $\delta = 4\alpha\gamma - \beta^2$. Hence if ω is an (α, β, γ)-number in an algebraic number field $\mathbf{\Omega}$, then $4\alpha\omega$ is a δ-number in $\mathbf{\Omega}$. Now there is a simple case when the converse is also true, i.e. if $4\alpha\omega$ is a δ-number in $\mathbf{\Omega}$ then ω is an (α, β, γ)-number in $\mathbf{\Omega}$.

Let $4\alpha\omega$ be a δ-number in $\mathbf{\Omega}$,

$$4\alpha\omega = \mu^2 + \delta\nu^2,$$

where μ and ν are integers in $\mathbf{\Omega}$. Then

$$(\mu + \beta\nu)(\mu - \beta\nu) = 4\alpha(\omega - \gamma\nu^2).$$

Obviously $\frac{1}{2}(\mu + \beta\nu)$ and $\frac{1}{2}(\mu - \beta\nu)$ are integers in $\mathbf{\Omega}$.

Now suppose the principal ideal (α) is a prime ideal in $\mathbf{\Omega}$. Then

$$\mu \pm \beta\nu \equiv 0 \pmod{2\alpha}$$

for one of the signs. For this sign we put

$$\mu \pm \beta\nu = 2\alpha\lambda$$

and obtain $$4\alpha\omega = (2\alpha\lambda \mp \beta\nu)^2 + (4\alpha\gamma - \beta^2)\nu^2$$

or $$\omega = \alpha\lambda^2 + \beta\lambda(\mp\nu) + \gamma(\mp\nu)^2.$$

Hence we have proved the following lemma.

Lemma 29. *If α is a prime in an algebraic number field Ω then an integer ω is an (α, β, γ)-number in Ω if and only if $4\alpha\omega$ is a δ-number in Ω, where $\delta = 4\alpha\gamma - \beta^2$.*

We now let Ω be the gaussian number field $\mathbf{K}(\sqrt{-1})$ and let D have one of the values 2, 3, 7, 11, 19, 43, 67 and 163. If α is a prime in $\mathbf{K}(\sqrt{-1})$ and $D = 4\alpha\gamma - \beta^2$ we then get the following characterization of (α, β, γ)-numbers in $\mathbf{K}(\sqrt{-1})$.

Theorem 11. *Let α, β and γ be integers in $\mathbf{K}(\sqrt{-1})$ such that α is a prime and $4\alpha\gamma - \beta^2 = D$, $D = 2, 3, 7, 11, 19, 43, 67$ or 163. Then an integer ω_0 in $\mathbf{K}(\sqrt{-1})$ is an (α, β, γ)-number in $\mathbf{K}(\sqrt{-1})$ if and only if $4\alpha\omega_0 = \omega$ satisfies the conditions to be a D-number in $\mathbf{K}(\sqrt{-1})$ stated in Theorems 6 B, 7 B, 8 B and 9 B.*

BIBLIOGRAPHY

1. Hasse, H. Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper. *J. reine angew. Math. 153* (1924), 113–130.
2. Hilbert, D. Über den Dirichletschen biquadratischen Zahlkörper. *Math. Ann. 45* (1894), 309–340 (*Gesammelte Abhandlungen* 1 (1932), 24–52).
3. ——, Über die Theorie des relativquadratischen Zahlkörpers. *Math. Ann. 51* (1889), 1–127 (*Gesammelte Abhandlungen* 1 (1932), 370–482).
4. Humbert, G. Sur la représentation d'un entier par les formes d'Hermite indéfinies, dans un corps quadratique imaginaire. *C. R. Acad. Sci. Paris 171* (1920), 287–293.
5. Jones, B. W. *The arithmetic theory of quadratic forms.* New York 1950.
6. Nagell, T. On the representations of integers as the sum of two integral squares in algebraic, mainly quadratic fields. *Nova Acta Soc. Sci. Upsal.* Ser. IV, Vol. 15, No. 11. Uppsala 1953.
7. ——, On the sum of two integral squares in certain quadratic fields. *Ark. Mat. 4* (1961), 267–286.
8. ——, On the number of representations of an A-number in an algebraic field. *Ark. Mat. 4* (1962), 467–478.
9. Siegel, C. L. Über die analytische Theorie der quadratischen Formen III. *Ann. of Math. 38* (1937), 212–291.
10. Speiser, A. *Die Theorie der binären quadratischen Formen mit Koeffizienten und Unbestimmten in einem beliebigen Zahlkörper.* Diss. Göttingen 1909.